IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s): B.M. Jakobsson et al.
Case: 22-2
Serial No.: 09/538,663
Filing Date: March 30, 2000
Group: 3693
Examiner: Stefanos Karmis

Title: Methods of Protecting Against Spam Electronic Mail

REPLY BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The remarks which follow are submitted in response to the Examiner's Answer dated April 21, 2008 in the above-identified application. The arguments presented by Appellants in the corresponding Appeal Brief are hereby incorporated by reference herein.

In the Answer at page 4, first paragraph, the Examiner indicates claims 18 and 20 as objected to. As acknowledged by the Examiner in an Advisory Action dated November 14, 2007, Appellants overcame these objections with an Amendment After Filing of Notice of Appeal Under 37 C.F.R. §41.33(a), dated September 20, 2007 and entered by the Examiner.

In the Answer at pages 8-13, the Examiner responds to various arguments raised by Appellants in the Appeal Brief.

Claims 1 and 10 (pages 8-9 of the Answer)

In page 8, third and fourth paragraphs, of the Answer, the Examiner asserts, *inter alia*, that "the teachings of Greenstein conform to the definition of a MAC as given in Appellant's specification as a secret password specific to the sender, receiver and the sent email . . . . because Greenstein teaches that the passcode is attached to a specific email and thus is specific to the email (column 2, lines 29-34)."

Appellants respectfully submit that the relied-upon portion of Greenstein teaches that "[w]hen sending an email, a sender must specify the passcode which was provided by the recipient and which is inserted in a predefined field in a mail header." However, Greenstein at column 2, lines 43-45, states that "a common passcode may be assigned to all senders, or alternately, individual passcodes may be given to each sender."

Thus, Greenstein teaches a technique wherein every email that a given sender sends to a given recipient will contain the same passcode; either the individual passcode given to that sender by the recipient or a common passcode assigned to all senders by the recipient. Appellants respectfully disagree with the Examiner's contention that a passcode which is identical in every email that a given sender sends to a given recipient is "a secret password specific to the sender, receiver and the sent email." Further support for Appellants' position may found in the specification at page 10, lines 10-13 ("An adversary will not be able to determine whether a given string is a valid MAC on a given message m unless the adversary obtains access to the given key. This is true even after an arbitrary number of MACs for chosen messages other than m have been examined by the adversary.")

With regard to the Examiner's contention that the present specification broadly defines a MAC as "a secret password specific to the sender, receiver and the sent email," Appellants respectfully note that the present specification at page 8, line 21, to page 9, line 5, states that a MAC "can be thought of as a secret password specific to the sender, receiver, and the sent email, and which only a sender who is registered can generate. More specifically, and as known in the art, a MAC is a keyed one-way function of an input wherein a secret key is known by both the generator and the verifier of the MAC." (emphasis added)

In page 9, first paragraph, of the Answer, the Examiner asserts that "all that is required by the claims . . . is 'MAC information.' Therefore, claims 1 and 10 do not even require a MAC, but instead just require at least some kind of 'information' associated with a MAC. Items such as the sender name, email address, time-stamp, recipient name, [and] recipient email address are types of 'information' used in the MAC. Greenstein teaches including attaching [sic] such information to the email (column 4, lines 27-43). Therefore, given its broadest reasonable interpretation, 'MAC information' is anticipated by Greenstein."

Applicants respectfully submit that it is axiomatic that the scope of claims in patent applications is to be determined "not solely on the basis of the claim language, but upon giving claims their broadest reasonable construction 'in light of the specification as it would be interpreted by one of ordinary skill in the art.'" *Phillips v. AWH Corp.*, 415 F.3d 1303, 1316, 75 USPQ2d 1321, 1329 (Fed. Cir. 2005) (citing *In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1364, 70 USPQ2d 1827 (Fed. Cir. 2004))

Appellants respectfully submit that the Examiner's interpretation of "MAC information" as being taught by Greenstein's disclosure of conventional e-mail header fields including "the sender name, email address, time-stamp, recipient name, [and] recipient email address" is inconsistent with the manner in which "MAC information" would be understood by one having skill in the art in light of the present specification at, for example, page 11, lines 16-20, and page 14, lines 1-12, which describe illustrative embodiments of the present invention in which MAC information is included as an extension of the recipient's email address or as an additional header of an email message.

Claims 17 and 19 (pages 9-10 of the Answer)

As a preliminary matter, Appellants note that, in page 9, third paragraph, of the Answer, the Examiner has mischaracterized claims 17 and 19 as independent claims, rather than dependent claims.

Claims 17 and 19 recite a limitation "wherein the particular sender becomes a registered sender by satisfying a requirement." In other words, claims 17 and 19 specify that the particular sender must satisfy a requirement to become a registered sender. As described in the present

specification at page 5, lines 6-11, in an illustrative embodiment, a "sender becomes a registered sender by paying a price which will allow the sender to become a registered sender to the receiver."

In formulating the rejection at page 9, last paragraph, of the Answer, the Examiner argues that "Greenstein teaches satisfying requirements because the seller must be welcomed, valid, or submit a request. All of these limitations satisfy a requirement to become pre-approved to send emails to the recipient." As noted above, claims 17 and 19 specify that the particular sender must satisfy a requirement to become a registered sender, not merely some vague concept of "satisfying a requirement," as the Examiner apparently alleges.

The Examiner relies primarily on portions of Greenstein which the Examiner characterizes as teaching that "all sellers must be pre-approved before they can send an email to the recipient (column 2, lines 15-20)," that a "user provides a passcode to all welcome email participants and maintains a list of valid senders (column 2, lines 25-30 [and column 4, lines 33-37])," and "that the sender can request a passcode (column 2, lines 59-63)."

Appellants respectfully submit that, even assuming the accuracy of the Examiner's characterizations of the relied-upon portions of Greenstein, Greenstein nonetheless fails to meet the limitation of claims 17 and 19 which specify that a particular sender must satisfy a requirement to become a registered sender.

For example, column 2, lines 15-20; column 2, lines 25-30; and column 4, lines 33-37, indicate that a recipient designates the seller as a valid sender. This does not indicate that the sender has satisfied a requirement, as required by claims 17 and 19; rather, a recipient may designate a sender as a valid sender regardless of whether the sender has satisfied any requirement.

Likewise, Greenstein's alleged teaching at column 2, lines 59-63 (emphasis added), "that the sender can request a passcode" clearly fails to disclose satisfying a requirement, as required by claims 17 and 19. Indeed, column 2, lines 59-63, merely indicate that the sender may request that the recipient designate the seller as a valid seller. Again, such designation does not indicate that the sender has satisfied a requirement, as required by claims 17 and 19; rather, a recipient

may designate a sender as a valid sender regardless of whether the sender has satisfied any requirement.

Claims 18 and 20 (pages 10-11 of the Answer)

As a preliminary matter, Appellants note that, in page 10, second paragraph, of the Answer, the Examiner has mischaracterized claims 18 and 20 as independent claims, rather than dependent claims. Claims 18 and 20 recite a limitation directed to "registering the particular sender when the particular sender is determined not to be a registered sender of email to the particular receiver."

In formulating the rejection at page 10, last paragraph, of the Answer, the Examiner contends that an "unregistered sender becomes registered when a passcode is received." Even assuming the accuracy of this contention, however, nowhere does Greenstein disclose the particular limitations of claims 18 and 20 wherein a particular sender is registered when the particular sender is determined not to be a registered sender of email to the particular receiver. Specifically, Greenstein fails to disclose providing a passcode to a sender when a sender is determined to be unregistered.

Rather, the Examiner relies on portions of Greenstein which the Examiner characterizes as teaching that "all sellers must be pre-approved before they can send an email to the recipient (column 2, lines 15-20)," that a "user provides a passcode to all welcome email participants and maintains a list of valid senders (column 2, lines 25-30 [and column 4, lines 33-37])," and "that the sender can request a passcode (column 2, lines 59-63)."

Appellants respectfully submit that these portions of Greenstein fail to disclose sending a passcode to a sender when a sender is determined to be unregistered. Rather, as noted above with regard to claims 17 and 19, these portions of Greenstein merely disclose that a recipient may designate the seller as a valid sender and that a sender can request a passcode. Nowhere do these portions of Greenstein teach providing a passcode to a sender when a sender is determined to be unregistered.

The Examiner further contends that "Greenstein teaches temporarily holding emails by senders who do not specify a passcode (i.e. not registered) and later decided to accept the email

(column 3, lines 52-67; Examiner notes this to be registering the sender when the email is approved)." Appellants respectfully submit that the relied-upon portion of Greenstein discloses a technique wherein, if a sender does not have a passcode, the user is prompted to authorize a single e-mail from the server, rather than providing a passcode to the sender (which the Examiner equates with registering the sender). See Greenstein at column 3, lines 52-61:

> At step 114, if a sender did not specify a passcode when sending to the user who requires such passcode, the server stores the e-mail in a temporary storage, i.e., a holding tank, at step 116. At step 118, the server transmits an authorization request to the user via the mail client, to either accept or reject the e-mail. If the user approves the e-mail at step 120, the e-mail is placed in the mail database at step 110, making it available to the mail client to retrieve at step 112. On the other hand, if the user rejects the e-mail at step 122, the e-mail is deleted at step 126.

Even if the user accepts the e-mail, the sender is not registered; rather, just that single e-mail will be delivered to the user. Unless the user provides a passcode to the sender, subsequent e-mails from that sender will also be stored in the temporary storage and require manual approval by the user prior to delivery. As such, Greenstein fails to disclose the limitations of claims 18 and 20.

Claims 3 and 11 (page 12 of the Answer)

Claims 3 and 11 each contain a limitation directed to "generating a pseudorandom function with a keyed hash function using an input number comprising a unique serial number for use in generating an identifier for email between the particular sender to the particular receiver."

In page 12, third paragraph, of the Answer, the Examiner argues that this limitation is met by Greenstein's teaching that a passcode may be "a randomly generated binary 'key'." The Examiner further argues that this "established passcode is an address associated with a particular receiver letting the sender know that the receiver desired that the sender be able to send emails to the recipient consistent with claim 2."

Appellants respectfully contend that the Examiner's explanation fails to indicate the manner in which Greenstein's passing mention of "a randomly generated binary 'key'" teaches or suggests a pseudorandom function with a keyed hash function using an input number comprising a unique serial number as recited in claims 3 and 11. Appellants further note that neither the Office Notice taken by the Examiner regarding the use of cookies nor the newly-cited Cockrill reference suggest, or indeed even mention, the use of a pseudorandom function with a keyed hash function using an input number comprising a unique serial number, and thus fail to remedy the fundamental deficiency of Greenstein to reach the limitations of claims 3 and 11.

Claim 12 (page 13 of the Answer)

Claim 12 recites a limitation wherein a registering module sets up an encrypted address for sending email from the particular receiver to the particular sender using public key encryption. As described with reference to an illustrative embodiment in the present specification at, for example, page 13, lines 5-7, "receiver R preferably adds redundancy to [the symmetric key selected by receiver R] by replying to sender S using a public extension on receiver R's address appended solely for the purposes of setup."

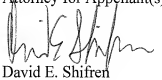
The Examiner contends that "the encrypted key taught by Kirsch qualifies as an encrypted address as it used when authenticating email from the sender to the recipient." Appellants respectfully submit that, even if Kirsch were considered to teach the use of an encrypted key when authenticating email from the sender to the recipient, such teachings would nevertheless fail to remedy the fundamental deficiency of Greenstein to reach the limitation of claim 12 directed to setting up an encrypted address for sending email from the particular receiver to the particular sender.

In view of the above, Appellants believe that claims 1-20 are in condition for allowance, and respectfully request the withdrawal of the present §102(e) and §103(a) rejections.

Respectfully submitted,

Date: April 21, 2008

Joseph B. Ryan
Reg. No. 37,922
Attorney for Appellant(s), by



David E. Shifren
Reg. No. 59,329
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-2641